Amendments to the Claims:

1. (Previously presented) A distributed system for monitoring a communications network and for detecting an unauthorized communications access attempt into the monitored communications network, the system comprising:

one or more distributed hierarchical monitoring systems; and

one or more alarm signals that represent an unauthorized communications access attempt into one or more portions of the monitored communications network,

wherein the one or more distributed hierarchical monitoring systems anal yze the unauthorized communications access attempt in response to the unauthorized communications access attempt, and determine a responsive action to the unauthorized communications access attempt, including sending a mechanism for determining a source of the unauthorized communications access attempt in a response to the unauthorized communications access attempt.

2. (Previously presented) The system of claim 1, further comprising a monitoring device that monitors information on one or more monitored communications networks.

3. (Previously presented) The system of claim 1, further comprising an intrusion analysis system that receives the one or more alarm signals and at least one of determines the origin of the unauthorized communications access attempt, logs communications and evaluates the threat of the unauthorized communications access attempt.

4. (Previously presented) The system of claim 1, further comprising an intrusion interaction system that is capable of communicating with the origin of the unauthorized communications access attempt.

5. (Previously presented) The system of claim 1, further comprising an escalation determination system that, based on an evaluation of the unauthorized communications access attempt and a comparison to one or more other unauthorized communications access

attempts, forwards information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

6. (Previously presented) The system of claim 1, wherein the one or more alarm signals is generated by one or more recipients of the unauthorized communications access attempt.

7. (Previously presented) The system of claim 1, further comprising a response system that communicates information regarding the unauthorized communications access attempt to one or more of a monitored site and a law enforcement agency.

8. (Previously presented) A method for monitoring a communications network and for detecting an unauthorized communications access attempt into the monitored communications network, the method comprising:

monitoring one or more portions of the monitored communications network through one or more distributed hierarchical monitoring systems; and

receiving one or more alarm signals that represent an unauthorized communications access attempt into one or more portions of the monitored communications network,

wherein the one or more distributed hierarchical monitoring systems anal yze the unauthorized communications access attempt in response to the unauthorized communications access attempt, and determine a responsive action to the unauthorized communications access attempt, including sending a mechanism for determining a source of the unauthorized communications access attempt in a response to the unauthorized communications access attempt.

9. (Previously presented) The method of claim 8, further comprising monitoring information relating to one or more geographic or organizational portions of the monitored communications networks.

10. (Previously presented) The method of claim 8, further comprising receiving the one or more alarm signals and at least one of determining the origin of the unauthorized

communications access attempt, logging communications and evaluating the threat of the unauthorized communications access attempt.

11. (Previously presented) The method of claim 10, wherein the logging can be restricted based on an analysis of the unauthorized communications access attempt.

12. (Previously presented) The method of claim 8, further comprising communicating with the origin of the unauthorized communications access attempt.

13. (Previously presented) The method of claim 8, further comprising forwarding, based on an evaluation of the unauthorized communications access attempt and a comparison to one or more other unauthorized communications access attempts, information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

14. (Previously presented) The method of claim 8, wherein the one or more alarm signals is generated by one or more recipients of the unauthorized communications access attempt.

15. (Previously presented) The method of claim 8, further comprising communicating information regarding the unauthorized communications access attempt to one or more of a monitored site and a law enforcement agency.

16. (Previously presented) The system of claim 1, wherein the one or more distributed hierarchical monitoring systems forward information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

17. (Previously presented) The system of claim 1, wherein the determining mechanism includes an identified packet concealed in the response, and the one or more distributed hierarchical monitoring systems detect passage of the identified packet.

18. (Previously presented) The system of claim 17, wherein the packet is identified by a flag, and the one or more distributed hierarchical monitoring systems detect passage of the flag.

19. (Previously presented) The system of claim 17, wherein the identified packet triggers reporting showing a path to the source of the unauthorized communications access attempt.

20. (Previously presented) The system of claim 1, wherein the determining mechanism includes a program concealed in the response.

21. (Previously presented) The system of claim 20, wherein the program is concealed in an HTML page sent as part of the response.

22. (Previously presented) The method of claim 8, wherein the one or more distributed hierarchical monitoring systems forward information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

23. (Previously presented) The method of claim 8, wherein the determining mechanism includes an identified packet concealed in the response, and the one or more distributed hierarchical monitoring systems detect passage of the identified packet.

24. (Previously presented) The method of claim 23, wherein the packet is identified by a flag, and the one or more distributed hierarchical monitoring systems detect passage of the flag.

25. (Previously presented) The method of claim 24, wherein the identified packet triggers reporting showing a path to the source of the unauthorized communications access attempt.

26 (Previously presented) The method of claim 8, wherein the determining mechanism includes a program concealed in the response.

27. (Previously presented) The method of claim 26, wherein the program is concealed in an HTML page sent as part of the response.

28. (Currently amended) [[A]] The method of claim 8, further comprising implementing said method via a computer program product including one or more computer-readable instructions configured to cause one or more computer processors to perform the steps ~~recited in claim 8~~ of the method.

29. (Previously presented) The system of claim 2, wherein the monitored information relates to one or more geographic or organizational portions of the monitored communications networks.